REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
05-04-2012	FINAL	

4. TITLE AND SUBTITLE

Social Media: Strategic Asset or Operational Vulnerability?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Charles Winchester, Major, USMC

Paper Advisors: Paul Povlock/John Kondratowicz, CAPT, USCG

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES: A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

At of the end of 2011, Facebook had 845 million monthly users, and these monthly users have the ability to communicate globally, share information instantly, and influence opinions. This ability to communicate globally, when viewed operationally, has caused social media to become another element of the joint operating environment and is something military commanders must consider as both an asset and a possible critical vulnerability. Left unchecked social media can be a critical strategic and operational vulnerability that can have an impact on operational success if it is not protected and used properly. Operational commanders must be aware of the advantages and disadvantages of social media and have safeguards in place to ensure it does not become a vulnerability. Social media is now part of the operating environment and should be considered alongside other operational functions when conducting planning.

15. SUBJECT TERMS

Social Media

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		23	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

SOCIAL MEDIA: STRATEGIC ASSET OR OPERATIONAL VULNERABILITY?

by

Charles P. Winchester

Major, U.S. Marine Corps

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

May 4, 2012

Abstract

At of the end of 2011, Facebook had 845 million monthly users, and these monthly users have the ability to communicate globally, share information instantly, and influence opinions. This ability to communicate globally, when viewed operationally, has caused social media to become another element of the joint operating environment and is something military commanders must consider as both an asset and a possible critical vulnerability. Left unchecked social media can be a critical strategic and operational vulnerability that can have an impact on operational success if it is not protected and used properly. Operational commanders must be aware of the advantages and disadvantages of social media and have safeguards in place to ensure it does not become a vulnerability. Social media is now part of the operating environment and should be considered alongside other operational functions when conducting planning.

Introduction

The internet and social media have become a global mainstay in the way people interact and communicate on a daily basis. With the constantly increasing capabilities of internet compatible electronic devices, such as cell phones, smart phones, and tablet personal computers, the global community has an expectation to be able to instantly communicate with family, friends, and colleagues, virtually unimpeded regardless of physical location. This ability to instantly and effectively communicate has not only benefited United States' service members and operational commanders, but has also benefited insurgent and terrorist organizations. This ability to communicate globally, when viewed operationally, has caused social media to become another element of the joint operating environment and is something military commanders must consider as both an asset and a possible critical vulnerability. Left unchecked social media can be a critical strategic and operational vulnerability that can have an impact on operational success if it is not protected and used properly. Operational commanders must be aware of the advantages and disadvantages of social media and have safeguards in place to ensure it does not become a vulnerability.

The internet and social media have created several advantages for both the general public and the military. Collaboration and information sharing has been made easier; data storage and instant access has created a repository of resources that can aid in decision making; and ease of communication throughout the globe has become the norm. Social media has even proven to be an asset during humanitarian assistance and disaster relief operations assisting both first responders and to inform the general public. Social media platforms, such as Facebook, MySpace, Twitter, and a host of others, are global and a factor of everyday life. For example, according to Facebook's official newsroom, as of December

31, 2011, there are 845 million monthly active users, with approximately 80 percent of active users living outside the United States and Canada.[1] With this amount of people using Facebook, the largest of the social media networks, there is the distinct possibility that it will be used for nefarious purposes. From an operational lens, with 845 million active users, news spreads quickly and globally, thereby potentially posing an operational and even strategic risk to military operations.

With continual advances in mobile technology, instant access will only continue to become more prevalent and an expectation. This instant access and the ability to globally communicate can serve many purposes in the military realm, such as keeping service members in touch with family members; allowing military commanders to communicate command specific announcements to unit members and family; and to inform the general public of military activities promoting transparency. The widespread use of social media is evident from a study cited by Dr. Mark Van Dyke on the U.S. Army's *DIME Blog* that reported "in an average 20 minute period in 2010 Facebook recorded 1,587,000 wall posts; 2,716,000 photo uploads; and 10,208,000 published comments." This same study reported that 46 percent of the world's population uses social media and 57 percent rely more on social media for social interaction than personal interaction or communication.[2]

Within the military, commanders are still seeking to harness social media as an outlet for messaging and command information. The issue becomes with so many people using social media, how can operational commanders harness this asset and prevent its intentional

1. Facebook Staff, "About Facebook," Facebook, accessed April 7, 2012, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.
2. Dr. Mark Van Dyke, "Social Media in the U.S. Military: A New Information Center of Gravity?" DIME Blog, accessed April 12, 2012, http://www.carlisle.army.mil/dime/blog/article.cfm?blog=dime&article=191.

or unintentional misuse? This includes protecting operational security and preventing inappropriate comments, photos, or posts. With many service members actively using multiple social media platforms, this is a challenge for all commanders from the tactical level up to the operational and strategic level. Social media is now part of the operating environment and should be considered alongside other operational functions when conducting planning.

Department of Defense Policies Regarding Internet Based Capabilities

From Facebook's inception in 2004 to early 2010, there existed no official Department of Defense (DoD) policy or guidance on the use of Facebook and other social media platforms. Specifically, policy was nonexistent on the usage of official government computers for accessing and acceptable content. Though no official policy existed, many government networks blocked access to social media type websites through the use of internet firewalls and other standard information assurance security protocols. Still the lack of official policy resulted in a haphazard and inconsistent approach to accessing social media platforms.

In June of 2009, Secretary of Defense Robert Gates cited the freedom of communications afforded by technology as a "huge strategic asset for the United States."[3] In this same press conference, Secretary Gates also conceded that "this department is way behind the power curve" with communications technology.[4] The Secretary understood the value of this type of communication and in August of 2009, the DoD directed a

3. Donna Miles, "Gates, Mullen: Communications Technologies 'Strategic Asset' for United States," U.S. Department of Defense, accessed April 5, 2012, http://www.defense.gov/news/newsarticle.aspx?id=54834.
4. Ibid.

comprehensive study of social media platforms to access the potential security risks.[5] The intent of this study was to try and balance the need for operational security with the growing use of social media by the members of the armed forces. It was understood that though social media can be a security risk in terms of operational security, it can also benefit the individual service member and the organization as a whole. The unstated benefit would be one of strategic communication with the American public by enabling public access to hear and see images from the individual service member, thereby telling the military story and garnering potential domestic support for the mission. If the American public could see and hear about the day-to-day activities and lives of the soldier, airman, sailor, or Marine, then the public would be more apt to trust the source since it would be perceived as firsthand knowledge.

The start of the DoD study resulted in a service wide ban on using social media via government computers, though as previously mentioned this ban was essentially in place through internet firewalls. For example in Marine Administrative Message 458/09, Headquarters Marine Corps implemented essentially a total ban on accessing social networking sites via the Marine Corps enterprise network, citing operational security and the possibility of malicious attack by outside actors.[6] This Marine Corps message indicated that social networking sites "are particularly high risk due to information exposure, user generated content, and targeting by adversaries."[7]

---

5. John Kruzel, "Pentagon Weighs Social Networking Benefits, Risks," U.S. Department of Defense, accessed April 5, 2012, http://www.defense.gov/news/newsarticle.aspx?id=55363.
6. Headquarters, U.S. Marine Corps, "*Immediate Ban of Internet Social Networking Sites on Marine Corps Enterprise Network NIPRNET*," U.S. Marine Corps, accessed April 3, 2012, http://www.marines.mil/news/messages/pages/maradmin0458-09.aspx.
7. Ibid.

The DoD study was completed in late 2009 and eventually resulted in publication of a DoD Directive Type Memorandum.[8] Published on February 25, 2010, this memorandum provided overarching policy and guidance on the use of social networking sites via the DoD's unclassified computer network. The memorandum provided guidance on official use of social networking sites as well as authorized use by service members to access social networking sites. The guidance stipulated that, "information posted must be relevant and accurate; include a disclaimer when personal opinions are expressed; and provide links to official DoD hosted content, when applicable."[9] The memorandum also stressed the use of operational security principles and the requirement for commanders at all levels to defend against potential malicious attacks. Shortly after the publication of this DoD directive memorandum, the services began publishing service specific guidance. For example, the Navy published guidance via an All Navy message and the Marine Corps did the same via a Marine Administrative Message. The Marine Corps message, published in March of 2010, reiterated much of the guidance published in the DoD memorandum, stressing appropriate content and detailing guidance on prohibited content (adult content, hate speech, gambling, etc.).[10] As is often the case in the military, once initial guidance is published on new trends, amplifying guidance soon follows and additional guidance can be expected as officials become more informed on the trend. This was the case with the Marine Corps. After publishing the March administrative message, the Marine Corps followed with a June message which provided social media guidance for Marines who, in their personal capacity,

8. U.S. Department of Defense, "*Responsible and Effective Use of Internet-based Capabilities*," DTM 09-026 (Washington, DC: Department of Defense, 25 February 2010).
9. Ibid.
10. Headquarters, U.S. Marine Corps, "*Responsible and Effective Use of Internet-based Capabilities*," U.S. Marine Corps, accessed April 8, 2012, http://www.marines.mil/news/messages/Pages/MARADMIN181-10.aspx.

desired to make official posts regarding service related topics.[11] This message recognized the value of social media as a tool for individual Marines to share the Marine Corps story with both domestic and foreign audiences and encouraged Marines to share personal experiences via this platform, but it also served as a warning to Marines about content. The message stated that individuals were responsible for all content they posted on the internet and the use of good, sound judgment should be the norm to refrain from inappropriate content that could bring discredit upon the individual, the unit, and the Marine Corps. This warning included both Marine Corps content and non-Marine related content. The unstated intent was to ensure Marines understood the permanency of the digital footprint.

When the DoD wide ban was lifted regarding social media access, the intent was to provide service members a way of communicating the military message to the public; provide a resource to stay connected with family members and friends; and simply serve as part of the overall DoD messaging mechanism. An additional consideration was the desire for DoD to leverage the benefits of social media. Much of the guidance that was published ensured operational security was not breeched; inappropriate content was not posted that would harm the reputation of the service; and stressed the importance of good judgment when posting information on the internet. The policy and guidance, though fairly specific, did not cover everything. The internet and social media have provided a venue for every service member to not only tell their personal military story, but also to potentially voice grievances, complaints, and inappropriate content. Publishing guidance and regulations covering every situation is impossible, but the initial training regarding the use of social

11. Headquarters, U.S. Marine Corps, "*Social Media Guidance-Unofficial Internet Posts*," U.S. Marine Corps, accessed April 4, 2012, http://www.marines.mil/news/messages/Pages/MARADMIN365-10.aspx.

media was strongly centered on operational security. This is partly evident in an interview the Master Chief Petty Officer of the Navy (MCPON) gave to Navy.mil. In this interview MCPON Rick West stated, "Operational security has to be stressed at every level and I'm going to make sure our Sailors understand that very clearly."[12] Though operational security should be stressed, the problem on the horizon was not only how does a commander train and educate subordinates on the importance of protecting operational security, but also how does the commander monitor subordinates' activities on social media to ensure compliance? How does a battalion commander monitor and provide oversight of social media networks for approximately 800 personnel?

As the use of social media matured, the services began looking at ways to embrace the technology and leverage it to spread command messages, service messages, and as an information sharing platform to include its use for family readiness. Over time social media guidance matured and many of the military services began to realize there was a need for overarching guidance and standardization. For example, in November 2010, the U.S. Army published a memorandum entitled *Standardizing Official U.S. Army External Official Presences (social media).*[13] This memorandum set to standardize social media presence throughout the U.S. Army. It listed ten standardized steps for commands to follow when establishing an official social media presence, to include registering the official page with the Office of the Chief of Public Affairs. The reasoning behind this memorandum was to establish uniformity in presence and design of all official U.S. Army social media sites. Additionally, in October 2011, the U.S. Army published the second version of *The United*

12. Senior Chief Bill Houlihan, "MCPON to Sailors: Be Smart about Online Threats," U.S. Navy, accessed April 3, 2012, www.navy.mil/search/display.asp?story_id=50411.
13. U.S. Army, "*Standardizing Official U.S. Army External Official Presences (social media)*," (Washington DC: Department of the Army, 1 November 2010).

States Army Social Media Handbook.[14] This 47 page document provided great detail to Army commands, and individual soldiers, on the proper use of social media. This handbook, published by the U.S. Army Office of Public Affairs, covered a wide variety of topics, to include privacy settings, operational security concerns, telling the Army story, and the use of social media for crisis communications. This handbook serves as a valuable resource for commanders in training and education of their soldiers. One of the key themes throughout this handbook is the proper use of social media and professional conduct. In the section entitled "Social Media Standards for Army Leaders," the Army, much like the Marine Corps, sent a message to leaders stating "conduct online should be professional." The handbook states, "By using social media, leaders are essentially providing a permanent record of what they say. If you would not say it in front of a formation, do not say it online."[15] Though standardization can be important, the simple fact is service members must be cognizance of what is posted online is permanent and can have secondary and tertiary effects.

The Marine Corps also published its version of a social media handbook entitled, "*The Social Corps*."[16] Like the U.S. Army handbook, the Marine Corps handbook covers many of the same topics. The handbook provides guidance on unofficial posts, personal safety issues such as privacy, operational security issues, and also has a section that provides guidance for families. The Marine Corps handbook also covers professional conduct and considerations to be aware of when posting personal opinions online; so much so that it is covered in multiple sections throughout the handbook. This is important because

14. U.S. Army, "*The United States Army Social Media Handbook*," (Washington DC: Department of the Army, October 2011).
15. Ibid.
16. Headquarters, U.S. Marine Corps, "*The Social Corps*," (Washington, DC: Marine Corps Production Directorate, date unknown).

professional conduct must be observed when using social media for either official or unofficial postings. The reputation of the services is generally measured by the conduct of the individual. A single unprofessional posting by an individual can have ramifications throughout the service and cause considerable damage to service reputation. This handbook is a valuable tool and provides information for every Marine that navigates the social media arena. The Marine Corps demonstrated its acceptance of social media as an asset through the establishment of its official presence on Facebook. Though the Marine Corps was the last service to enter the social media space, it was the first official DoD page to exceed one million fans.[17]

There are other guidelines and handbooks regarding social media, to include a handbook prepared by Facebook entitled, "*Building Your Presence with Facebook Pages: A Guide for Military Organizations*." At the combatant command level, Central Command has a section on its official website regarding Facebook presence and the dangers associated with operating in the online environment. These handbooks are important training aids and provide ample guidance regarding appropriate content, professionalism, operational security concerns, and covers the associated benefits of social media. From publishing the handbooks to the prevalence of United States military organizations developing official Facebook and other social media pages, it is readily apparent that the military is accepting social media.

17. Cpl Scott Schmidt, "*Marines Innovate to Stay Relevant, Surpass 1 Million Fans on Facebook*," U.S. Marine Corps, accessed April 8, 2012, www.marines.mil/unit/hqmc/pages/marines-innovate-to-stay-relevant-surpass-1-million-fans-on-facebook.

Advantages of Social Media

There are many advantages to using social media, to include personal, professional, and organizational. There are also advantages at the tactical, operational, and strategic levels of command.

At the personal/individual level, social media allows for constant communication with loved ones and provides family and friends an update on events that are going on in one's life. This provides the opportunity to build personal connections. A soldier deployed to Afghanistan has the ability to post on Facebook events that are happening half a world away from his family and friends. On some level this provides a personal connection to the current war in Afghanistan and can have the secondary effect of keeping a community connected to the sacrifices and dangers soldiers face every day. This connection allows an individual soldier to tell his Army story and influence local and possibly national public opinion about the military mission. It is a form of strategic communication that if used properly can provide needed support for strategic policy. This personal interaction with friends and family on the home front can also be a morale booster for those deployed. If used improperly and outside established guidelines, the results can be disastrous. For instance, a service member's first stop to voice a grievance or dissatisfaction about policy or operations should not be social media. There are other procedures in place for grievances and voicing them through social media is not one of them.

Professionally, social media can be used as a conduit for specific groups of people. For example, a regimental commander can form a social media group that only serves his battalion commanders. Only commanders would have access to this group and it would be kept private from other viewers. Obviously this would all have to be at the unclassified level,

but it can serve as a method to share best practices for training, discipline, or a host of other topics. It can also serve as a platform for the regimental commander to share his commander's intent or guidance and basically just a tool for information sharing. This type of group sharing can apply to any functional community within the military. Disbursing, platoon commanders, administrators, logisticians, and many more can benefit from this type of community knowledge sharing. One potential issue with using social media in this manner is there already exist many internet based applications that already do this. For example, many commands have an intranet portal, Microsoft SharePoint software, networked computer drives, and public folders via Microsoft Outlook. The issue is with so many venues and platforms available to share information, which one should be used? Additionally, this information can be shared in personal social settings, such as officers' call or other types of gatherings. Where social media may be valuable is when commanders are not co-located in the same geographical area, such as a wing commander located in Cherry Point, North Carolina who has subordinate squadrons at Marine Corps Air Station Beaufort, South Carolina. The problem is with so many computer and internet applications available for information collaboration, who manages the information to ensure it is all in one place, and the right place?

Organizationally, social media can be beneficial in terms of command messaging, family readiness, calendars, and even recruiting. For example, many commands and organizations have Facebook pages, Twitter accounts, web pages, and so forth that are used to provide news feeds of command activities, useful family readiness information, possibly a commander's newsletter, or a calendar of events. These types of sites are invaluable tools in keeping the public and family members informed, while adding a level of transparency to

unit activities. From a recruiting perspective, all the military services are active on Facebook and most have Twitter feeds. Using Facebook helps the services reach the target market demographic of the 18-24 year old, as social media is where this market tends to get their information. Senior leaders from the services have also engaged social media to reach a wider audience. For example, the most junior soldier in the U.S. Army can view the Army Chief of Staff's, General Ray Odierno, Facebook page. Social media provides General Odierno the ability to spread his guidance to a wider audience than he could ever reach in person.[18] The Sergeant Major of the Army, Raymond Chandler, has also embraced social media. From a senior enlisted advisor position he is able to quickly spread information regarding new Army guidance, but more importantly he uses his social media presence to generate and facilitate discussions that are germane to the junior soldier.[19] The military's most senior leader, Chairman of the Joint Chiefs of Staff, General Martin Dempsey, USA, uses his Facebook page to tell the military's story. The key to senior leader engagement with social media is to stay relevant, stay current, and stay engaged with those they serve. If senior leaders are personally managing their Facebook pages, specifically the comments, they need to ensure they are sending the right message and attempting to target the right audience. Staying current with information posted on Facebook can give the page creditability. They must also review their personal Facebook pages and respond to posts as appropriate. Responding to posts and comments from friends or the public at large makes the receiver feel a connection to the originator.[20]

18. U.S. Army, "*The United States Army Social Media Handbook*," (Washington DC: Department of the Army, October 2011), 18.
19. Ibid, 18.
20. Ibid, 7.

For social media to be an asset to commanders and senior leaders it must be thought of as any other military piece of equipment. Failure to become proficient, or knowledgeable, in the operation of social media, or failure to understand the social impact of the messages that are posted can negate the potential impact. If a soldier is not proficient in the operation of his personal weapon, then the soldier is ineffective on the battlefield. The same can be said for any military occupational specialty; if one is not technically proficient in the execution of their duties, then the military is not leveraging an asset. Commands, commanders, and senior leaders can be virtually present within many forms of social media and have access to a wide audience, but if they fail to keep their messages current, relevant, and stay engaged with their audience, then the use of social media as an asset will be a failure. This does not imply that commanders have to personally perform these functions, but it does imply commander involvement and oversight at some level. Much of this can be delegated with guidance and direction from the commander.

Social media is an interactive platform. What this generally means is there is a continuous back and forth type dialogue on social media. Comments are posted, questions are asked, and then questions are answered. A virtual conversation takes place. When there is a lack of response to questions asked by an individual poster, commands and leaders lose an opportunity. This can be especially important in an operational setting. If commands and leaders in an operating environment are posting information, but not responding to comments, then the command's social media page can be viewed as irrelevant or just as another government information machine. Using social media as an operational communication tool means administrators of the social media site have to stay engaged their

audience.[21] This is one of the underlying problems with the military and the ability to exploit social media; it is generally used as a public affairs asset and not leveraged as an interactive communication tool. Simply reviewing both Central Command and the International Security Assistance Force (ISAF)-Afghanistan's Facebook pages lends credence to this impression. Both pages are full of public affairs type information, with news stories and photos which are telling the story, but there is no credible engagement with those who are posting comments. Additionally, activity counts on either page are less than 6000.[22] With 845 million monthly Facebook users there is potential to engage a much wider audience.

DISADVANTAGES OF SOCIAL MEDIA

"Technology used to give us Kodak moments, and now technology gives us stupidity at the speed of light. The great challenge that this poses is that imagery is not in the hands of a few. It is in the hands of everybody".
Doug Wilson, Assistant Secretary of Defense for Public Affairs

Assistant Secretary Wilson's warning came shortly after a video appeared on the internet of Marines allegedly urinating on dead Taliban fighters. The underlying message is that with the current technology everyone has the ability to influence messaging, perception, public opinion, and possibility the mission. Technology, and specifically social media, has outpaced military guidance, training, and enforcement. There are numerous examples of "bad social media" that have impacted operations, public perception, and had unintended consequences.

21. Headquarters, U.S. Marine Corps, "*The Social Corps*," (Washington, DC: Marine Corps Production Directorate, date unknown), 23.
22. ISAF: NATO Forces in Afghanistan, http://www.facebook.com/ISAF (accessed April 12, 2012).

The most infamous incident is the Abu Ghraib prisoner abuse that came to public attention in 2004.[23] This incident, though not specifically tied to social media such as Facebook, was tied to the internet and demonstrated how fast a bad incident could spread. The swiftness that this story spread and the second and third order effects of the images permanently on the internet, and in the hands of terrorists looking for sympathy or recruits, had the effect of undermining hundreds of thousands of service members' efforts in Iraq.

More recently, the video of Marines allegedly urinating on dead Taliban is another example of bad judgment on the part of young service members. From a cursory check of YouTube, and totaling only three separate postings of this video, this 42-second video has garnered 1,653,126 views.[24] These 1.6+ million viewers are from all around the globe and have differing views and opinions regarding the United States and efforts to defeat terrorism. This video serves only to damage American image and reputation throughout the world and it is now part of the internet permanent record and can potentially be used by adversaries to discredit ISAF-Afghanistan efforts. Additionally, once the video went viral it served to divert the attention of senior leadership from the task of combating terrorism to one of answering questions regarding the actions of four Marines who exercised poor judgment.

Another disadvantage of social media is it is susceptible to hacking just like any other computer based system. In 2011, a hacking incident involving U.S. Navy Admiral James Stavridis resulted in senior British officials unintentionally disclosing personal information to

23. Rebecca Leung, "Abuse of Iraqi POWs by GIs Probed," CBS News, April 29, 2004, http://www.cbsnews.com/stories/2004/04/27/60ii/main614063.shtml.
24. "Marines Urinate on Taliban," accessed April 8, 2012, http://www.youtube.com/watch?v=SljHO-b4YEs.

unknown individuals.[25] This incident demonstrates only one of the vulnerabilities of social media. People operating in the social media environment are unseen and often times rely on the complacency of individuals they are attempting to target. Hackers will set up fake profiles in an attempt to solicit information from unsuspecting individuals hoping there will not be an attempt to verify authenticity. This poses a vulnerability that commanders need to be aware of in order to take the necessary precautionary steps.

There are many more examples of social media gone badly and all generally have one common thread: the poor judgment of the individual posting the information. Given the demographics of the U.S. military, with approximately 44 percent in the 17-24 age bracket, commanders and senior leaders have cause for concern when it comes to social media.[26] This is the generation that grew up in the internet age and is accustomed to posting anything and everything on the internet for the world to see. As this generation matures in their military service they will become the new strategic corporals.

The military has always referenced the importance of the strategic corporal and defined the term as a young person who has the ability to make decisions that can potentially have tactical, operational, and strategic implications. This is largely in reference to the operating environment and how senior leaders cannot be everywhere on the battlefield. The term was coined by Marine Commandant, General Charles Krulak, in 1999 and appeared in an article he wrote for *Marines Magazine* in January 1999 emphasizing the need to develop young leaders who can make decisions in a complex operating environment. The military

25. Emil Protalinski, "Chinese Spies Use Fake Facebook Profile to Friend NATO Officials," accessed April 5, 2012, http://www.zdnet.com/blog/facebook/chinese-spies-use-face-facebook-profile-to-friend-nato-officials.
26. U.S. Department of Defense, "*Population Representation in the Military Services FY10*," (Washington, DC: Department of Defense, 25 February 2011).

still has the strategic corporal, except now that corporal has access to Facebook, MySpace, Twitter, and has a smart phone to take photos. How does the military ensure the new generation of strategic corporals make the right decisions when it comes to social media and the posting of comments and photos on the internet?

Conclusion

Military commanders and senior leaders have taken small steps in harnessing social media, but there is more to be done. Social media can have positive effects both on the home front and in an operating environment and it has to be used as more than a tool to post news stories. Commanders, or those delegated the responsibility, have to be engaged with social media and the content that is published, as well as engaged with their audiences. In order to fully leverage social media, commanders have to be trained on its use and its potential impacts, just as they would be trained on any other new weapon.

Commanders can avoid the adverse implications of the strategic corporal unintentionally, or intentionally, posting inappropriate content by conducting indoctrination about the dangers and potential implications of inappropriate content early, and often, in the training pipeline. This could be started as early as when an individual enlists in the delayed entry program. In addition to mental and physical preparedness for recruit training, young enlistees should begin receiving training on ethics, to include proper conduct on social media as it relates to being a member of the profession of arms. This training must continue at recruit training, to include an introduction and overview of the services' social media handbooks. Training on social media should be reinforced through the curriculums of the services' leadership schools targeting mid-grade and senior level enlisted and officer leaders. Without continually training and reinforcement of the training, nothing will change.

Social media can provide many benefits to commanders, but there has to be supervision, oversight, commander guidance, and enforcement. It is now part of the operating environment and must be considered as both an asset and potential vulnerability. It is a responsibility of all leaders to ensure subordinates understand what is to be accomplished via social media and to establish guidelines concerning content. It is up to the individual service member to exercise good judgment when posting either official or unofficial content on the internet. The expectations need to be explained, reinforced, and individuals must be held accountable for their actions.

Bibliography

Elliott, Stuart. "Army Seeks Recruits in Social Media." *New York Times.* May 24, 2011. http://www.nytimes.com/2011/05/25/business/media/25adco.html?_r=3

Facebook. "Building Your Presence with Facebook: A Guide for Military Organizations." undated. http://www.facebook.com/usmilitary (accessed April 2, 2012).

—. Facebook Newsroom. December 31, 2011. http://newsroom.fb.com/content/default.aspx?NewsAreald=22 (accessed April 7, 2012).

Headquarters, U.S. Marine Corps. *Immediate Ban of Internet Social Networking Sites on Marine Corps Enterprise Network NIPRNET.* August 3, 2009. http://www.marines.mil/news/messages/pages/maradmin0458-09.aspx (accessed April 4, 2012).

—. *Responsible and Effective Use of Internet-Based Capabilities.* March 29, 2010. http://www.marines.mil/news/messages/Pages/MARADMIN181-10.aspx (accessed April 7, 2012).

—. *Social Media Guidance-Unofficial Posts.* June 29, 2010. http://www.marines.mil/news/messages/Pages/MARADMIN365-10.aspx (accessed April 5, 2012).

Hoskinson, Charles. "DOD: Phones Can't Outsmart Troops." January 18, 2012. www.politico.com/news/stories/0112/71626.htmlCached (accessed April 5, 2012).

Houlihan, Bill. "MCPON to Sailors: Be Smart about Online Threats," U.S. Navy, January 6, 2012, www.navy.mil/search/display.asp?story_id=50411 (accessed April 3, 2012).

ISAF-Afghanistant. *ISAF: NATO Forces in Afghanistan.* 2012. http://www.facebook.com/ISAF (accessed April 12, 2012).

Kruzel, John J. *Pentagon Weighs Social Networking Benefits, Risks.* August 4, 2009. http://www.defense.gov/news/newsarticle.aspx/id=55363 (accessed April 4, 2012).

Leung, Rebecca. "Abuse of Iraqi POWs by GIs Probed," CBS News, April 29, 2004, http://www.cbsnews.com/stories/2004/04/27/60ii/main614063.shtml.

Marines Urinate on Taliban, accessed April 8, 2012, http://www.youtube.com/watch?v=SljHO-b4YEs (accessed April 8, 2012).

Miles, Donna. *Gates, Mullen: Communications Technologies 'Strategic Asset' for United States.* June 18, 2009. http://www.defense.gov/news/newsarticle.aspx?id=54834 (accessed April 5, 2012).

—. "Iraq Social Media Experience Sparks Training for Leaders." July 30, 2009. http://www.defense.gov/news/newsarticle.aspx?id=55321.

Montalbano, Elizabeth. "Army: Social Network Geotagging Puts Soldiers At Risk." March 13, 2012. http://www.informationweek.com/news/government.

Protalinski, Emil. "Chinese Spies Used Fake Facebook Profile to Friend NATO Officials." March 11, 2012. http://www.zdnet.com/blog/facebook/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials (accessed April 5, 2012).

Rodewig, Cheryl. "Social Media Misuse Punishable Under UCMJ." February 9, 2012. http://www.army.mil/article/73367/social_media_punishable_under_ucmj/

Schmidt, Scott Cpl. "Marines Innovate To Stay Relevant, Surpass 1 Million Fans on Facebook." March 3, 2011. http://www.marines.mil/unit/hqmc/marines-innovate-to-stay-relevant-surpass-1-million-fans-on-facebook (accessed April 8, 2012).

U.S. Army. "Standarizing Official U.S. Army External Official Presences (Social Media)." November 1, 2010. www.carlisle.army.mil/dime/getDoc.cfm?fileID=452 (accessed April 5, 2012).

—. "The United States Army Social Media Handbook." October 2011. http://www.army.mil/socialmedia (accessed March 25, 2012).

U.S. Central Command. "FAQ on Security for Social Media." unknown. http://www.centcom.mil/faq-on-security-for-social-media (accessed April 5, 2012).

U.S. Department of Defense. "Population Representation in the Military Services." February 2011. http://prhome.defense.gov/RFM/MPP/ACCESSION%20POLICY/PopRep2010/index.html (accessed April 10, 2012).

—. "Responsible and Effective Use of Internet-based Capabilities." February 25, 2010. http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf (accessed April 3, 2012)

U.S. Navy. *MCPON to Sailors: Be Smart about Online Threats.* January 6, 2010. www.navy.mil/search/display.asp?story_id=50411 (accessed April 7, 2012).

Wohlsen, Marcus. "US Seeks to Mine Social Media to Predict Future." February13, 2012. http://www.military.com/news/article/us-seeks-to-mine-social-media-to-predict-future.html.

Montalbano, Elizabeth. "Army: Social Network Geotagging Puts Soldiers At Risk." March 13, 2012. http://www.informationweek.com/news/government.